Seoul Design Foundation

" 시민과 함께하는 청렴재단 "

17년 서울디자인재단 통합보안장비 UTM (Unified Threat Management) 운영 결과보고

2017. 12. 22.

문서번호	전산정보팀-1873
결재일자	2017.12.28.
공개여부	비공개(7)
방침번호	대표이사방침 제1536호

선임	전산정보팀장	운영본부장	DDP경영단장	대표이사	
12/22 김찬란	12/22 노태화	12/27 강문석	12/27 유석윤	12/28 이근	
협 조					

추진근거	- 16년 서울디자인재단 정보시스템 통합 운영 및 유지관리 사업 계획(대표이사방침 제1888호, 2016.06.27.) - 17년 서울디자인재단 통합보안장비 UTM(Unified Threat Management) 운영계획(안)(대표이사방침 제 3562호, 2016.11.25.) - 17~18년 서울디자인재단 정보시스템 통합 운영 및 유지관리 사업 계획(대표이사방침 제 2258호, 2017.06.08.)		
대 내 외 협력현황	부서(단체)명	협의내용	협의결과
	-	-	-
사 업 비	17년 10,296천원		

서울디자인재단 (전산정보팀)

사전 검토항목

※ 해당사항이 없을 경우 '무 ✔' 표시하시기 바랍니다.

검 토 항 목	검토여부 '✔' 표시					
시 민 참 여 고 려 사 항	시 민 :	유 □ ( )	무 ✔			
	이 해 당 사 자 :	유 □ ( )	무 ✔			
	전 문 가 :	유 □ ( )	무 ✔			
	옴 브 즈 만 :	유 □ ( )	무 ✔			
법령및기타 고 려 사 항	법 령 규 정 :	교통 □	환경 □	재해 □	기타 ✔	무 □
	기 타 :	고용효과 □	노동인지 □	균형인지 □		
		취약계층 □	성인지 □	장애인 □	디자인 □	
		갈등발생 가능성 □	유지관리 비용 ✔	무 □		
타 자 원 의 활 용	중 앙 부 처 :	유 □ ( )	무 ✔			
	민 간 단 체 :	유 □ ( )	무 ✔			
	기 업 :	유 □ ( )	무 ✔			
관 계 기 관 및 단체 협의	관 계 기 관 :	유 □ ( )	무 ✔			
	관 련 단 체 :	유 □ ( )	무 ✔			

17년 서울디자인재단 통합보안장비
UTM(Unified Threat Management) 운영 결과보고

17년 서울디자인재단 정보시스템의 보안 및 네트워크 안정성을 위한 통합보안장비(UTM) 운영 결과를 보고하고자 함.

1. 2017년 결과 요약

■ 운영개요

□ 운영 대상 : 통합보안장비(UTM) 에스원 정보보안솔루션

- 기기명: 에스원NS(MF2 500 중형)
- 규격: TSN0202

□ 운영 기간 : 17. 1. 1. ~ 17.12.31.

□ 운영 방향 : ① 시스템 자원 현황 분석 ② 사이버 유해 공격 탐지 및 차단 ③ 재단 보안 안정성 유지

■ 결과 요약

연번	구분		세부내역	
1	월평균 보안상태 (상태)		안전	
2	월평균 시스템 자원 사용 현황 (%)	CPU	30	
		메모리	60	
		디스크	86	
3	IPS 및 외부공격 탐지/차단 (건수)	IPS/DDoS	총합	12,727,505
			월평균	1,157,045
		불법URL	총합	3,474
			월평균	315
		웹악성코드	총합	2,177
			월평균	917
4	어플리케이션 제어 (건수)		총합	2,047,279
			월평균	186,116

5 운영 개선사항

구분	장비 대여	모니터링	침입위험 알림	월간 레포트	사용자 지원
16년 렌탈	O	업무시간	X	X	X
17년 렌탈 및 관제	O	24시간	O	O	O

[참고] 주요 경과사항

□ '15년도 재단 정보시스템 사업계획 수립

- 재단 정보시스템 유지보수 사업 추진계획(단장방침 제964호, '15. 3.30)

□ '15년 서울디자인재단 통합보안장비(UTM) 임대 및 유지보수(1년차)

- 사업기간 : '15. 4 ~ '15.12(총 9개월)
- 계약기간 : '15. 4. 3 ~ '18. 4. 2(약정기간 3년)
- 위치: 서울디자인지원센터 1층 전산실

□ 16년 서울디자인재단 통합보안장비 UTM 운영계획 수립

- '16년 서울디자인재단 통합보안장비 UTM(Unified Threat Management) 운영계획(본부장방침 제 79호, 2016.02.11.)

□ '16년 서울디자인재단 통합보안장비(UTM) 임대 및 유지보수(2년차)

- 사업기간 : '16. 1 ~ '16. 12(총 12개월)
- 총 사업비 : 7,896,000원(VAT 포함)

□ 17년 서울디자인재단 통합보안장비 UTM 운영계획 수립

- '17년 서울디자인재단 통합보안장비 UTM(Unified Threat Management) 운영계획(안)(대표이사방침 제3562호, 2016.11.28.)

2. 세부 내용

■ 운영대상

□ 대상장비 : 에스원NS(MF2 500 중형)

[참고] 장비 세부정보

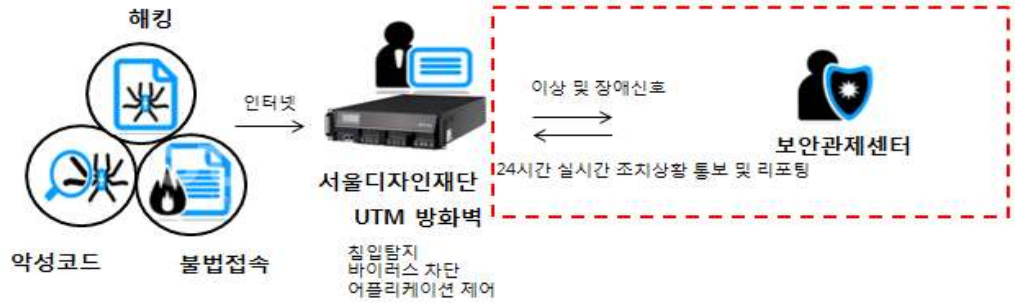
구분	상 세 내 용
사양	· CPU : 2.6GHz(2core) · Memory : 4GB · HDD : 250GB · CF Memory : 2GB · Power : 이중화 지원 안함 · NIC : 1GC * 6
N/W성능	· CPS : 80,000 · Concurrent Session : 1,500,000
F/W성능	· F/W Throughput : 2Gbps · Max 정책 : 5,000
VPN 성능	· VPN Throughput : 0.7Gbps · VPN Tunnels : 5,000 · SSL VPN 동시 사용자 : 100명
IPS 성능	· IPS Throughput : 1.1Gbps
인증	· 국가정보원 CC인증 EAL 4 · TTA Verified IPv6 인증 · IPv6 Ready Logo 인증 · 그린IT 구현을 위한 RoHS 충족
사진	

■ 운영개선 사항

□ 16년 및 17년 보안운영 전후 비교

16년

17년



■ 운영내용

연번	구분	세부내역
1	웹 필터링 / URL 차단	- 우회 접속 및 유해 사이트 차단 - 방송통신위원회 제공 DB 업데이트
2	IPS / DDos	- 해킹시도 및 웜 트래픽 패턴 분석 및 차단 - Anti-DDos전용장비 엔진 적용 ※ DDos :Distribute Denial of Service, 분산서비스거부 - 내부 좀비 PC 모니터링 및 차단 기능 - 가상 보호 도메인에 대한 보호 및 보안 정책의 적용
3	안티 바이러스	- 실시간 바이러스 감지 및 차단 - 바이러스 DB 자동 업데이트
4	취약점 진단	- 취약점 점검 툴을 사용하여 내부 자원의 취약점 파악 - 점검 결과를 설정에 적용하여 최적화된 보안정책 유지
5	애플리케이션 제어	- http/https를 이용하는 다양한 인터넷 애플리케이션 제어 - 애플리케이션별 User ID로 행위 제어
6	보안 정책 관리	- 연관 정책관리로 효율적인 보안정책 관리
7	NS 관제	- 보안장비 대여 및 유지보수 진행 - 실시간 원격 관제를 통한 보안정책 설정지원, 장애대응 등 모니터링 - 침입, 바이러스/스팸, 유해사이트 차단현황 정보 제공

■ 세부 운영결과

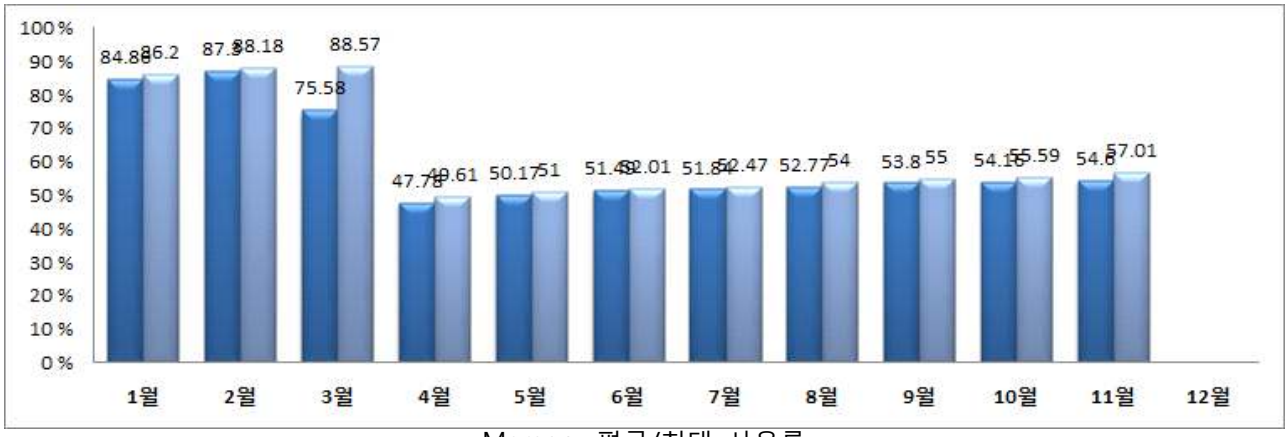
1. 보안상태

구분	보안상태	비고
1월	안전	
2월	안전	
3월	안전	
4월	안전	
5월	안전	
6월	안전	
7월	안전	
8월	안전	
9월	안전	
10월	안전	
11월	안전	

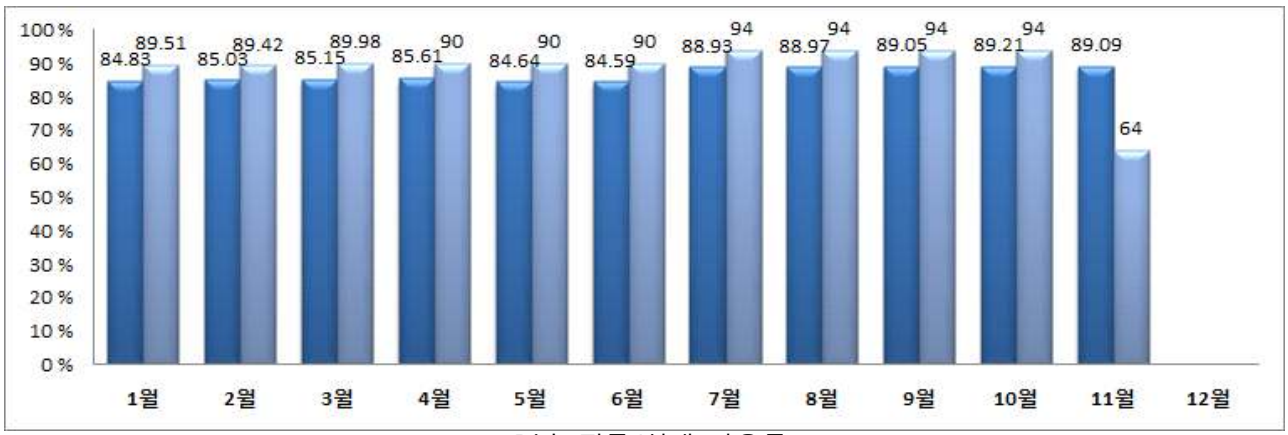
2. 시스템 자원 사용 현황

구분	CPU(%)		Memory(%)		디스크(%)		비고
	평균	최대	평균	최대	평균	최대	
1월	48.2	55.63	84.86	86.2	84.83	89.51	
2월	49.46	55.87	87.3	88.18	85.03	89.42	
3월	33.41	56.05	75.58	88.57	85.15	89.98	
4월	24.54	30.33	47.78	49.61	85.61	90.0	
5월	23.85	27.43	50.17	51.0	84.64	90.0	
6월	24.24	27.16	51.49	52.01	84.59	90.0	
7월	28.65	39.84	51.84	52.47	88.93	94.0	
8월	26.21	30.84	52.77	54.0	88.97	94.0	
9월	25.11	27.9	53.8	55.0	89.05	94.0	
10월	24.48	27.82	54.16	55.59	89.21	94.0	
11월	25.28	30.59	54.6	57.01	89.09	64.0	

CPU 평균/최대 사용률



Memory 평균/최대 사용률



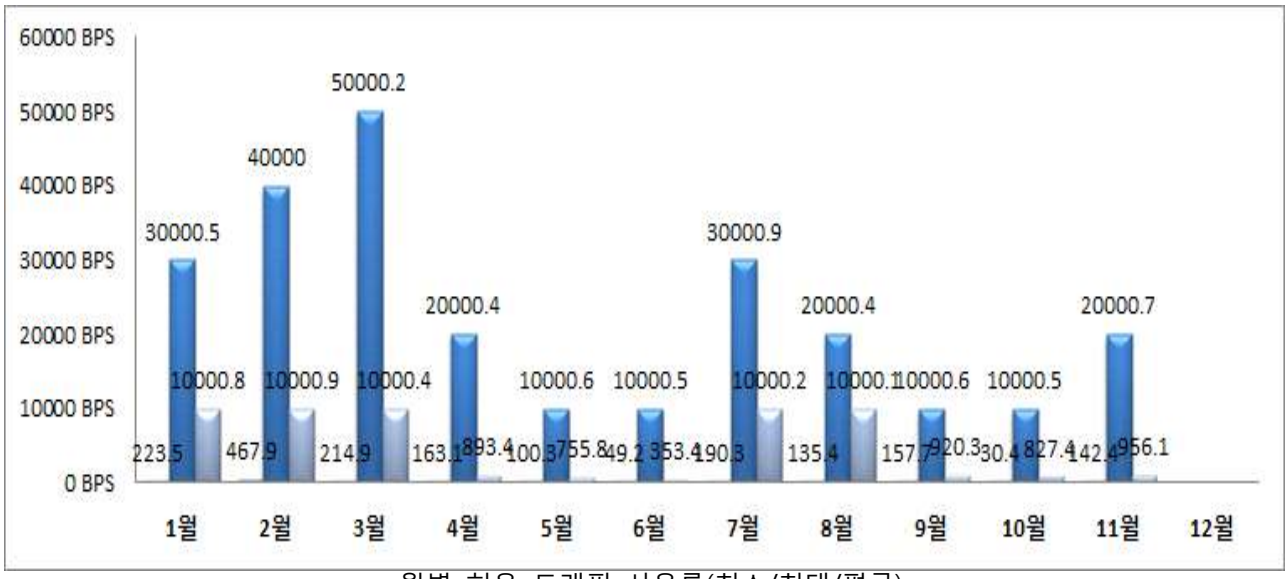
Disk 평균/최대 사용률

3. 월별 허용 트래픽 현황

※ 트래픽 : 서버에 전송되는 모든 통신 및 데이터의 양

구분	전체 허용 트래픽(BPS)			비고
	최소 트래픽	최대 트래픽	평균 트래픽	
1월	223.5K	3.5M	1.8M	
2월	467.9K	4M	1.9M	
3월	214.9K	5.2M	1.4M	
4월	163.1K	2.4M	893.4K	
5월	100.3K	1.6M	755.8K	
6월	49.2K	1.5M	353.4K	
7월	190.3K	3.9M	1.2M	
8월	135.4K	2.4M	1.1M	
9월	157.7K	1.6M	920.3K	
10월	30.4K	1.5M	827.4K	
11월	142.4K	2.7M	956.1K	

※ BPS : Bits Per Second



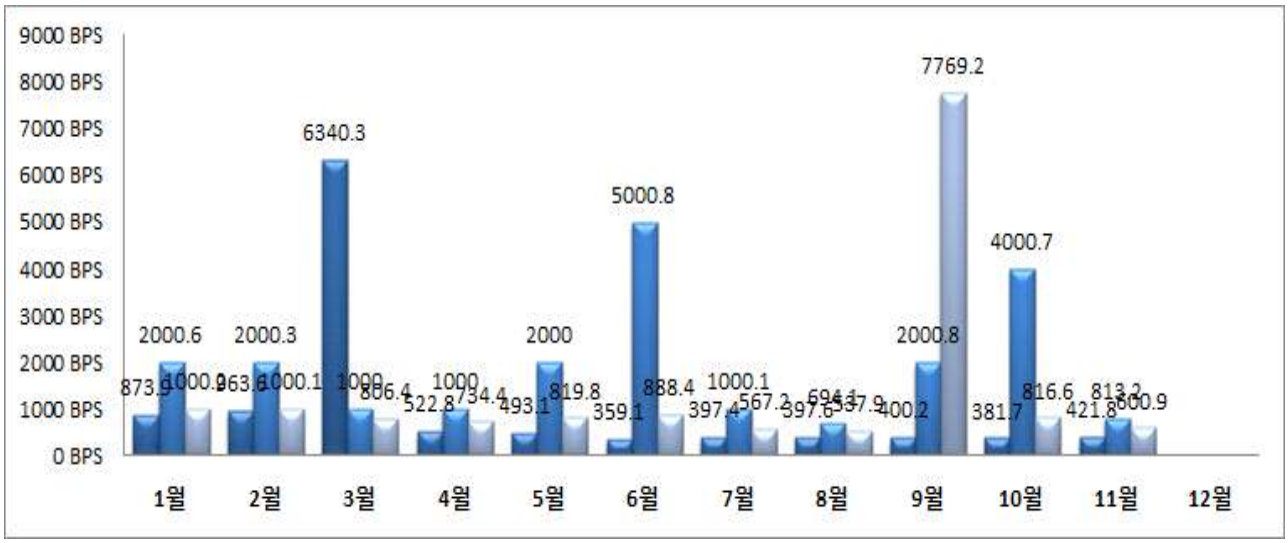
월별 허용 트래픽 사용률(최소/최대/평균)

4. 월별 거부 트래픽 현황

※ 트래픽 : 서버에 전송되는 모든 통신, 데이터의 양

구분	전체 거부 트래픽(BPS)			비고
	최소 트래픽	최대 트래픽	평균 트래픽	
1월	873.9	2.6K	1.2K	
2월	963.6	2.3K	1.1K	
3월	634.3K	1K	806.4	
4월	522.8	1K	734.4	
5월	493.1	2K	819.8	
6월	359.1	5.8K	888.4	
7월	397.4	1.1K	567.2	
8월	397.6	694.1	537.9	
9월	400.2	2.8K	7769.2	
10월	381.7	4.7K	816.6	
11월	421.8	813.2	600.9	

※ BPS : Bits Per Second



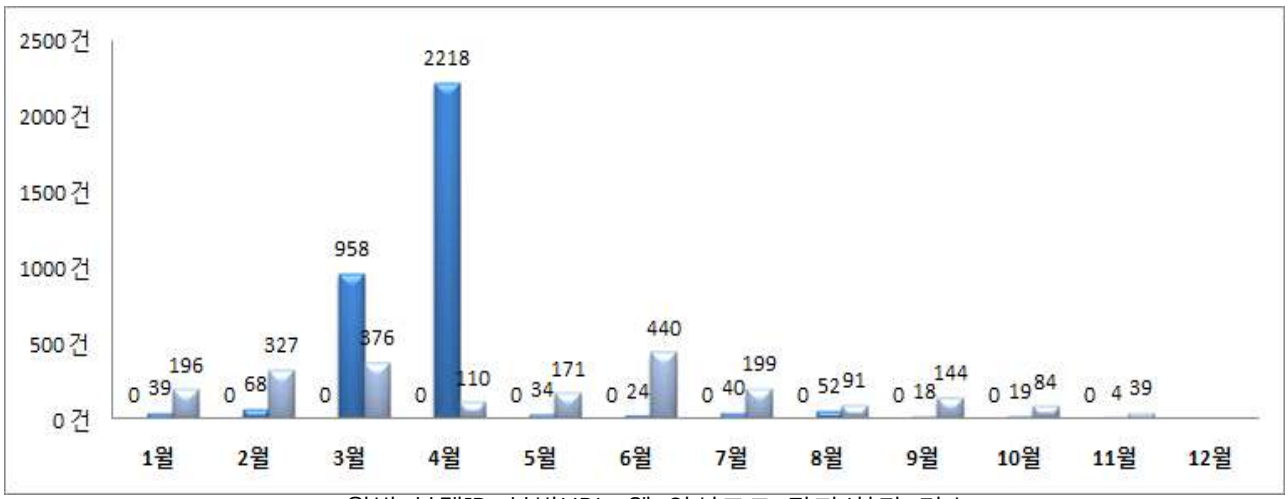
월별 허용 트래픽 사용률(최소/최대/평균)

5. 월별 IPS 및 외부공격 탐지/차단 현황

※ 침입방지 시스템 IPS(Intrusion Prevention System) : 네트워크 상에 공격하려는 대상을 찾아 자동 예방함으로 비정상적 트래픽을 중단시키는 보안 솔루션

구분	탐지/차단건수 IPS/DDoS	블랙리스트 유해IP 차단	불법URL 차단건수	웹악성코드 차단건수	비고
1월	1219476	0	39	196	
2월	1227871	0	68	327	
3월	1321059	0	958	376	
4월	1410324	0	2218	110	
5월	1490567	0	34	171	
6월	1269426	0	24	440	
7월	1167529	0	40	199	
8월	1214929	0	52	91	
9월	798040	0	18	144	
10월	789733	0	19	84	
11월	818551	0	4	39	

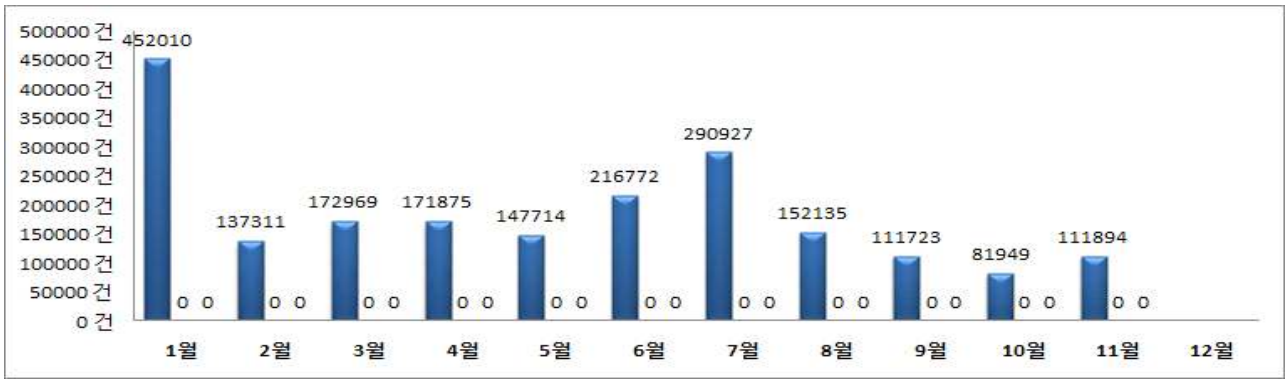
월별 IPS/DDoS 탐지/차단 건수



월별 블랙IP, 불법URL, 웹 악성코드 탐지/차단 건수

6. 월별 어플리케이션 및 외부공격 탐지/차단 현황

구분	어플리케이션 제어	바이러스 및 악성코드 탐지/차단	광고, 음란메일 불필요메일 차단	비고
1월	452010	0	0	
2월	137311	0	0	
3월	172969	0	0	
4월	171875	0	0	
5월	147714	0	0	
6월	216772	0	0	
7월	290927	0	0	
8월	152135	0	0	
9월	111723	0	0	
10월	81949	0	0	
11월	111894	0	0	



월별 어플리케이션, 바이러스/악성코드, 스팸메일 탐지/차단 건수

■ 기대효과

□ UTM 보안장비를 활용한 네트워크 보안 강화

□ 17년 운영개선 및 전문업체 유지보수를 통한 시스템 성능 최적화

□ 유지보수체제는 24시간 최적의 상태에서 정상적으로 운용

3. 소요 예산

■ 소요예산 : 10,296천원(VAT 포함, 12개월)

■ 예산과목 : 재단, 일반관리비, 운영경비, 운영경비, 수선유지비

4. 향후 계획

■ 18. 1 ~ 18. 3 : 4년차 UTM 임대 및 유지보수

■ 18. 3: 임대계약 연장 또는 구매 검토 ※ 세부 실행 상황에 따라 일정은 변경 가능

붙임 : 1. '17년 서울디자인재단 통합보안장비 UTM(Unified Threat Management) 운영계획 1부.
2. 서울디자인재단 전산장비 임대 및 유지보수(UTM) 계약서 1부. 끝.